

(19) 日本国特許庁 (JP)

## (12) 公開特許公報(A)

(11) 特許出願公開番号

特開2005-45756

(P2005-45756A)

(43) 公開日 平成17年2月17日 (2005.2.17)

(51) Int.Cl. <sup>7</sup>	F I	テーマコード (参考)
H04L 9/00	H04L 9/00 601C	5B017
G06F 12/14	G06F 12/14 320E	5B085
G06F 15/00	G06F 15/00 330Z	5D044
G09C 1/00	G09C 1/00 640E	5J104
G11B 20/10	G11B 20/10 D	
審査請求 未請求 請求項の数 31 O L (全 28 頁) 最終頁に続く		

(21) 出願番号 特願2003-406359 (P2003-406359)  
 (22) 出願日 平成15年12月4日 (2003.12.4)  
 (31) 優先権主張番号 特願2003-194491 (P2003-194491)  
 (32) 優先日 平成15年7月9日 (2003.7.9)  
 (33) 優先権主張国 日本国 (JP)

(71) 出願人 000003078  
 株式会社東芝  
 東京都港区芝浦一丁目1番1号  
 (74) 代理人 100075812  
 弁理士 吉武 賢次  
 (74) 代理人 100088889  
 弁理士 橋谷 英俊  
 (74) 代理人 100082991  
 弁理士 佐藤 泰和  
 (74) 代理人 100096921  
 弁理士 吉元 弘  
 (74) 代理人 100103263  
 弁理士 川崎 康

最終頁に続く

(54) 【発明の名称】 情報通信装置、通信システム及びデータ伝送制御プログラム

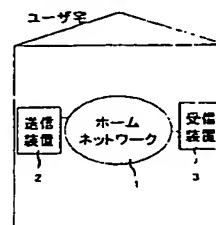
## (57) 【要約】

【課題】 著作権保護を図りつつ、著作権保護の必要な電子データを有効利用できるようにする。

【解決手段】 本発明に係る通信システムは、個人宅内で主にAVデータを送受信することを目的としており、ホームネットワーク1に接続された送信装置2及び受信装置3を備えている。デバイスIDの登録要求を行ってから所定時間以内に応答が返ってきた場合のみ、他の通信装置（受信装置3または送信装置2）の登録を行うようにしたため、有限の範囲内の通信装置との間でのみAVデータの伝送を行うことができ、簡易な処理でAVデータの著作権保護を図ることができる。

【選択図】 図1

図1の発明形態の概略構成



## 【特許請求の範囲】

## 【請求項 1】

他の通信装置との間で、著作権保護のための暗号化された電子データを伝送する情報通信装置において、

ネットワークを介して取得した前記他の通信装置の装置識別情報を登録する識別情報管理手段と、

前記他の通信装置が予め定めた距離的な条件を満たす場合、または前記他の通信装置と共通の識別情報を携帯装置から受信した場合に、該他の通信装置の装置識別情報を前記識別情報管理手段に登録する制御を行う事前登録手段と、

前記識別情報管理手段に登録されている装置識別情報を持つ前記他の通信装置との間で、著作権保護のための認証鍵交換を行う認証鍵交換処理手段と、を備えることを特徴とする情報通信装置。

10

## 【請求項 2】

他の通信装置に対して、著作権保護のための暗号化された電子データを送信する情報通信装置において、

ネットワークを介して取得した前記他の通信装置の装置識別情報を登録する識別情報管理手段と、

前記他の通信装置が所定の有限範囲内のネットワークに接続されていると認識した場合に、該他の通信装置の装置識別情報を前記識別情報管理手段に登録する制御を行う事前登録手段と、

20

前記識別情報管理手段に登録されている装置識別情報を持つ前記他の通信装置との間で、著作権保護のための認証鍵交換を行う認証鍵交換処理手段と、を備えることを特徴とする情報通信装置。

## 【請求項 3】

他の通信装置から送信された、著作権保護のための暗号化された電子データを受信する情報通信装置において、

ネットワークを介して取得した前記他の通信装置の装置識別情報を登録する識別情報管理手段と、

前記他の通信装置が所定の有限範囲内のネットワークに接続されていると認識した場合に、該他の通信装置の装置識別情報を前記識別情報管理手段に登録する制御を行う事前登録手段と、

30

前記識別情報管理手段に登録されている装置識別情報を持つ前記他の通信装置との間で、著作権保護のための認証鍵交換を行う認証鍵交換処理手段と、を備えることを特徴とする情報通信装置。

## 【請求項 4】

ローカルネットワークに接続されたインターフェース手段を備え、

前記事前登録手段は、前記他の通信装置が前記ローカルネットワークに直接接続されている場合に、該他の通信装置の装置識別情報を前記識別情報管理手段に登録することを特徴とする請求項 2 または 3 に記載の情報通信装置。

## 【請求項 5】

前記他の通信装置に対して装置識別情報の送信要求を行ってから、該他の通信装置からの装置識別情報が受信されるまでの時間が予め定めた時間以内か否かを判断する応答時間判断手段を備え、

40

前記事前登録手段は、前記応答時間判断手段により前記時間以内と判断された場合に、前記他の通信装置の装置識別情報を登録することを特徴とする請求項 2 乃至 4 のいずれかに記載の情報通信装置。

## 【請求項 6】

前記識別情報管理手段に登録された装置識別情報の数が予め定めた上限数に達した場合には、前記事前登録手段は、それ以上の装置識別情報の登録を拒絶するか、もしくは最も古くに登録された装置識別情報と最も長い間通信を行っていない他の通信装置の装置識別

50

情報との少なくとも一方を削除した上で、新たな装置識別情報を登録することを特徴とする請求項2乃至5のいずれかに記載の情報通信装置。

【請求項7】

前記他の通信装置からの認証・鍵交換要求を受信する認証・鍵交換要求受信手段を備え

、  
前記事前登録手段は、前記認証・鍵交換要求受信手段で認証・鍵交換要求が受信された後に、前記他の通信装置の装置識別情報を前記識別情報管理手段に登録する制御を行うことを特徴とする請求項2乃至6のいずれかに記載の情報通信装置。

【請求項8】

前記事前登録手段は、前記他の通信装置の装置識別情報を前記識別情報管理手段に登録する制御を、データリンクレイヤフレームまたは物理レイヤフレームにて行うことを特徴とする請求項2乃至7のいずれかに記載の情報通信装置。

【請求項9】

前記認証・鍵交換処理手段による認証鍵交換に成功した場合に、前記他の通信装置との間で前記電子データをやり取りする制御を行うデータ伝送処理手段を備え、

前記認証・鍵交換処理手段及び前記データ伝送処理手段は、IP (Internet Protocol) パケットを用いて各処理を行うことを特徴とする請求項2乃至8のいずれかに記載の情報通信装置。

【請求項10】

送信装置と、

前記送信装置から送信された、著作権保護のための暗号化を行った電子データを受信する受信装置と、を備える通信システムにおいて、

前記送信装置及び前記受信装置の少なくとも一方は、

ネットワークを介して取得した他方の装置の装置識別情報を登録する識別情報管理手段と、

前記他方の装置が所定の有限範囲内のネットワークに接続されていると認識できる場合に、該他方の装置の装置識別情報を前記識別情報管理手段に登録する制御を行う事前登録手段と、

前記識別情報管理手段に登録されている装置識別情報を持つ前記他方の装置との間で、著作権保護のための認証鍵交換を行う認証鍵交換処理手段と、を備えることを特徴とする通信システム。

【請求項11】

送信装置と、前記送信装置から送信された著作権保護のための暗号化を行った電子データを受信する受信装置と、の間で、電子データを伝送する制御を行うデータ伝送制御プログラムにおいて、

ネットワークを介して取得した前記他の通信装置の装置識別情報を登録するステップと

、  
前記他の通信装置が所定の有限範囲内のネットワークに接続されていると認識できる場合に、該他の通信装置の装置識別情報を前記識別情報管理手段に登録する制御を行うステップと、

前記識別情報管理手段に登録されている装置識別情報を持つ前記他の通信装置との間で、著作権保護のための認証鍵交換を行う認証鍵交換処理手段と、を実行させるための伝送制御プログラム。

【請求項12】

ネットワークを介して他の通信装置に対して、著作権保護のための暗号化された電子データを送信する情報通信装置において、

識別情報送信装置との間で、前記ネットワークとは異なるインタフェースを介して通信を行い、前記識別情報送信装置から送信された固有の識別情報を受信する通信手段と、

受信された前記固有の識別情報を登録する識別情報登録手段と、

前記他の通信装置が前記固有の識別情報を登録しているか否かを判断する識別情報登録

10

20

30

40

50

判断手段と、

前記他の通信装置が前記固有の識別情報を登録していると判断される場合に、該他の通信装置との間で、著作権保護のための認証鍵交換を完了させる第1の認証鍵交換処理手段と、を備えることを特徴とする情報通信装置。

【請求項13】

他の通信装置からネットワークを介して送信された、著作権保護のための暗号化された電子データを受信する情報通信装置において、

識別情報送信装置との間で、前記ネットワークとは異なるインタフェースを介して通信を行い、前記識別情報送信装置から送信された固有の識別情報を受信する通信手段と、

受信された前記固有の識別情報を登録する識別情報登録手段と、

前記他の通信装置が前記固有の識別情報を登録しているか否かを判断する識別情報登録判断手段と、

前記他の通信装置が前記固有の識別情報を登録していると判断される場合に、該他の通信装置との間で、著作権保護のための認証鍵交換を完了させる第1の認証鍵交換処理手段と、を備えることを特徴とする情報通信装置。

【請求項14】

前記暗号化された電子データを受信する入力処理手段と、

前記入力処理手段で受信された電子データを、復号した後に出力する出力処理手段と、を備えることを特徴とする請求項13に記載の情報通信装置。

【請求項15】

前記固有の識別情報の登録開始を指示する登録開始指示手段をさらに備え、

前記識別情報登録手段は、前記登録開始指示手段による指示があった場合に、登録処理を行うことを特徴とする請求項12乃至14のいずれかに記載の情報通信装置。

【請求項16】

前記登録開始指示手段による指示があった場合に前記通信手段に電源電圧を供給する電源制御手段をさらに備えることを特徴とする請求項15に記載の情報通信装置。

【請求項17】

前記通信手段を介して、前記識別情報送信装置との間で認証鍵交換を行う第2の認証鍵交換処理手段をさらに備え、

前記識別情報登録手段は、前記第2の認証鍵交換処理手段による認証鍵交換に成功した場合に、登録処理を行うことを特徴とする請求項12乃至16のいずれかに記載の情報通信装置。

【請求項18】

前記識別情報送信装置に対して特定のパケットを送信し、これに対する前記識別情報送信装置からの応答パケットが返ってくるまでのラウンドトリップ時間を計測する計測手段を備え、

前記第2の認証鍵交換処理手段は、前記計測手段で計測されたラウンドトリップ時間が所定時間以下の場合に認証鍵交換を行うことを特徴とする請求項17に記載の情報通信装置。

【請求項19】

前記計測手段によるラウンドトリップ時間の計測が終了した後に、前記識別情報登録手段による処理を開始することを特徴とする請求項18に記載の情報通信装置。

【請求項20】

前記識別情報登録手段が前記固有の識別情報を登録した旨を通知する登録通知手段をさらに備えることを特徴とする請求項12～19のいずれかに記載の情報通信装置。

【請求項21】

前記通信手段で受信された前記固有の識別情報を暗号化する暗号化手段と、

前記暗号化手段で暗号化された前記固有の識別情報を前記識別情報登録手段に伝送する暗号化情報伝送手段と、をさらに備えることを特徴とする請求項12乃至20のいずれかに記載の情報通信装置。

## 【請求項 22】

前記固有の識別情報は、個々の前記識別情報送信装置に固有のものであることを特徴とする請求項 12 乃至 21 のいずれかに記載の情報通信装置。

## 【請求項 23】

前記識別情報登録手段は、互いに異なる前記固有の識別情報の登録数を、予め定めた所定数以下に制限することを特徴とする請求項 12 乃至 22 のいずれかに記載の情報通信装置。

## 【請求項 24】

ネットワークを介して著作権保護のための暗号化された電子データを伝送する第 1 及び第 2 の通信装置に対して、識別情報を送信する情報通信装置であって、

前記第 1 及び第 2 の通信装置が前記電子データを伝送するのに必要な固有の識別情報を保持する識別情報保持手段と、

前記第 1 及び第 2 の通信装置に対して前記固有の識別情報を送信する通信手段と、を備えることを特徴とする情報通信装置。

## 【請求項 25】

前記識別情報保持手段は、保持可能な識別情報の数を所定個に制限することを特徴とする請求項 24 に記載の情報通信装置。

## 【請求項 26】

前記通信手段は、赤外線を用いて前記第 1 及び第 2 の通信装置の間で無線通信を行うことを特徴とする請求項 24 または 25 に記載の情報通信装置。

## 【請求項 27】

前記通信手段は、双方向の赤外線通信手段であり、

前記通信手段とは別個に、片方向の赤外線通信を行う片方向通信手段をさらに備えることを特徴とする請求項 26 に記載の情報通信装置。

## 【請求項 28】

前記通信手段は、受信電波により生成された電力を利用して前記第 1 及び第 2 の通信装置の間で無線通信を行うことを特徴とする請求項 24 または 25 に記載の情報通信装置。

## 【請求項 29】

前記通信手段は、着脱可能な記憶装置を用いて、前記第 1 及び第 2 の通信装置の間で通信を行うことを特徴とする請求項 24 または 25 に記載の情報通信装置。

## 【請求項 30】

ネットワークに接続された送信装置と、

前記送信装置から送信された、著作権保護のための暗号化を行った電子データを、前記ネットワークを介して受信する受信装置と、を備える通信システムにおいて、

前記送信装置及び前記受信装置の少なくとも一方は、

識別情報送信装置との間で、前記ネットワークとは異なるインタフェースを介して通信を行い、前記識別情報送信装置から送信された固有の識別情報を受信する通信手段と、

受信された前記固有の識別情報を登録する識別情報登録手段と、

前記他の通信装置が前記固有の識別情報を登録しているか否かを判断する識別情報登録判断手段と、

前記他の通信装置が前記固有の識別情報を登録していると判断される場合に、該他の通信装置との間で、著作権保護のための認証鍵交換を完了させる認証鍵交換処理手段と、を備えることを特徴とする通信システム。

## 【請求項 31】

ネットワークに接続された送信装置と、前記送信装置から送信された、著作権保護のための暗号化を行った電子データを前記ネットワークを介して受信する受信装置と、の間で、電子データを伝送する制御を行うデータ伝送制御プログラムにおいて、

識別情報送信装置との間で、前記ネットワークとは異なるインタフェースを介して通信を行い、前記識別情報送信装置から送信された固有の識別情報を受信するステップと、

受信された前記固有の識別情報を登録するステップと、

前記他の通信装置が前記固有の識別情報を登録しているか否かを判断するステップと、前記他の通信装置が前記固有の識別情報を登録していると判断される場合に、該他の通信装置との間で、著作権保護のための認証鍵交換を完了させるステップと、を実行させるためのデータ伝送制御プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、送信装置と受信装置との間で、著作権保護を図る必要のある電子データを送受信する情報通信装置、通信システム及びデータ伝送制御プログラムに関する。

【従来の技術】

10

【0002】

デジタル情報家電と呼ばれる商品が増加している。これら商品は、デジタル放送の開始などに伴って普及が期待されており、デジタル放送対応テレビやセットトップボックス、デジタルVTR、DVDプレーヤ、ハードディスクレコーダなどのデジタルデータやデジタルコンテンツを扱う種々の商品が含まれている。

【0003】

これら商品の普及に伴って考慮すべき問題の一つはコンテンツの著作権保護である。デジタルデータは、コピー時の品質劣化がないなどの利点がある一方で、不正コピーが容易であるなどの欠点がある。

【0004】

20

このため、デジタルAV機器同士をつなぐデジタルネットワークであるIEEE1394には、認証・鍵交換機能やデータの暗号化の機能が設けられている。

【0005】

ここで、ある送信装置から著作権保護が必要なAVデータを受信装置に伝送する場合を想定する。この場合、注意すべきことは、個人（あるいは、拡大解釈して家族）の楽しむ範囲内でAVデータをやり取りするのが著作権保護の前提であり、他人間間でのAVデータのやり取りは、視聴料や著作権料等の支払等が伴わない限り、行うべきではないという点である。

【0006】

ネットワーク上で著作権保護を図る仕組みとして、DTCP (Digital Transmission Content Protection) が知られている。DTCPは、IEEE1394やUSBなどでデファクトスタンダードになっている著作権保護方式である。DTCPでは、著作権保護が必要なAVデータなどのコンテンツに対して、送信装置と受信装置との間で認証・鍵交換処理を行い、AVデータを暗号化して伝送する（非特許文献1参照）。

30

【0007】

一般に、伝送系における著作権保護では、以下の処理手順でAVデータを伝送する。

【0008】

まず、送信装置と受信装置との間で、AVデータを送受信するためのコマンドを発行する。例えば、AV制御コマンドの一つである再生コマンドを、受信装置が送信装置に対して発行する。

40

【0009】

次に、AVデータに対して著作権保護のための暗号化を施した上で、送信装置から受信装置に対してAVデータの転送を始め、それに前後して、送信装置と受信装置との間で、著作権保護のための認証・鍵交換処理を行う。

【0010】

認証・鍵交換処理に成功すると、送信装置と受信装置との間でAVデータの暗号鍵を共有できるようになるか、あるいは送信装置と受信装置が暗号鍵を計算できるようになり、受信装置は受信した暗号化AVデータの復号及び再生を行う。

【0011】

AVデータの転送を、IP(インターネットプロトコル)上にて行うようにすれば、ウェブ等

50

の様々なアプリケーションと連携でき、ウェブブラウザ等の資産も活用でき、種々のネットワーク形態に対応させることもできる。

【0012】

このため、MPEG等で圧縮されたAVデータを伝送するプロトコルとして、IP（より具体的には、IPv4またはIPv6）を用いることが多い。より具体的なプロトコルとしては、例えばRTP(Real Time Transport Protocol)やHTTP(Hyper Text Transport Protocol)が用いられる。

【非特許文献1】 <http://www.dtcp.com>

【発明の開示】

【発明が解決しようとする課題】

10

【0013】

しかしながら、IPでは、具体的なネットワークの形態に関係なく、IPパケットを伝送できるため、セキュリティ上問題が生じる。すなわち、IPには、VPN(Virtual Private Network: 仮想プライベートネットワーク)といった、遠隔のIPネットワーク同士を論理的に接続する技術がある。この技術を用いると、例えばA地区のXさん宅のホームネットワークと、(A地区とは物理的に離れた)B地区のYさん宅のホームネットワークを論理的に接続し、この上でIPパケットの転送が可能となる。つまり、Xさん宅のホームネットワークとYさん宅のホームネットワークとが、あたかも1つのホームネットワークであるかのような形でネットワークの運用が可能である。

【0014】

20

著作権法等では、「個人の楽しむ範囲内」でのAVデータのコピー等は許容されているが、「他人同士」のコピー等は許容していない。しかし、上記のような技術(例えばVPN技術)を用いることにより、「他人同士のネットワークでも、論理的に1つのネットワークであると見せかけること(構成すること)」が可能になり、著作権法等に違反する機器を提供してしまうおそれがある。

【0015】

本発明は、このような点に鑑みてなされたものであり、その目的は、著作権保護を図りつつ、著作権保護の必要な電子データを有効利用できるようにした情報通信装置、通信システム及びデータ伝送制御プログラムを提供することにある。

【課題を解決するための手段】

30

【0016】

上述した課題を解決するために、本発明は、他の通信装置との間で、著作権保護のための暗号化された電子データを伝送する情報通信装置において、ネットワークを介して取得した前記他の通信装置の装置識別情報を登録する識別情報管理手段と、前記他の通信装置が予め定めた距離的な条件を満たす場合、または前記他の通信装置と共通の識別情報を携帯装置から受信した場合に、該他の通信装置の装置識別情報を前記識別情報管理手段に登録する制御を行う事前登録手段と、前記識別情報管理手段に登録されている装置識別情報を持つ前記他の通信装置との間で、著作権保護のための認証鍵交換を行う認証鍵交換処理手段と、を備える。

【0017】

40

また、本発明は、他の通信装置に対して、著作権保護のための暗号化された電子データを送信する情報通信装置において、ネットワークを介して取得した前記他の通信装置の装置識別情報を登録する識別情報管理手段と、前記他の通信装置が所定の有限範囲内のネットワークに接続されていると認識した場合に、該他の通信装置の装置識別情報を前記識別情報管理手段に登録する制御を行う事前登録手段と、前記識別情報管理手段に登録されている装置識別情報を持つ前記他の通信装置との間で、著作権保護のための認証鍵交換を行う認証鍵交換処理手段と、を備える。

【0018】

また、本発明は、他の通信装置から送信された、著作権保護のための暗号化された電子データを受信する情報通信装置において、ネットワークを介して取得した前記他の通信装

50

置の装置識別情報を登録する識別情報管理手段と、前記他の通信装置が所定の有限範囲内のネットワークに接続されていると認識した場合に、該他の通信装置の装置識別情報を前記識別情報管理手段に登録する制御を行う事前登録手段と、前記識別情報管理手段に登録されている装置識別情報を持つ前記他の通信装置との間で、著作権保護のための認証鍵交換を行う認証鍵交換処理手段と、を備える。

【0019】

また、本発明は、送信装置と、前記送信装置から送信された、著作権保護のための暗号化を行った電子データを受信する受信装置と、を備える通信システムにおいて、前記送信装置及び前記受信装置の少なくとも一方は、ネットワークを介して取得した他方の装置の装置識別情報を登録する識別情報管理手段と、前記他方の装置が所定の有限範囲内のネットワークに接続されていると認識できる場合に、該他方の装置の装置識別情報を前記識別情報管理手段に登録する制御を行う事前登録手段と、前記識別情報管理手段に登録されている装置識別情報を持つ前記他方の装置との間で、著作権保護のための認証鍵交換を行う認証鍵交換処理手段と、を備える。

10

【0020】

また、本発明は、ネットワークを介して他の通信装置に対して、著作権保護のための暗号化された電子データを送信する情報通信装置において、識別情報送信装置との間で、前記ネットワークとは異なるインタフェースを介して通信を行い、前記識別情報送信装置から送信された固有の識別情報を受信する通信手段と、受信された前記固有の識別情報を登録する識別情報登録手段と、前記他の通信装置が前記固有の識別情報を登録しているか否かを判断する識別情報登録判断手段と、前記他の通信装置が前記固有の識別情報を登録していると判断される場合に、該他の通信装置との間で、著作権保護のための認証鍵交換を完了させる第1の認証鍵交換処理手段と、を備える。

20

【0021】

また、本発明は、他の通信装置からネットワークを介して送信された、著作権保護のための暗号化された電子データを受信する情報通信装置において、識別情報送信装置との間で、前記ネットワークとは異なるインタフェースを介して通信を行い、前記識別情報送信装置から送信された固有の識別情報を受信する通信手段と、受信された前記固有の識別情報を登録する識別情報登録手段と、前記他の通信装置が前記固有の識別情報を登録しているか否かを判断する識別情報登録判断手段と、前記他の通信装置が前記固有の識別情報を登録していると判断される場合に、該他の通信装置との間で、著作権保護のための認証鍵交換を完了させる第1の認証鍵交換処理手段と、を備える。

30

【0022】

また、本発明は、ネットワークを介して著作権保護のための暗号化された電子データを伝送する第1及び第2の通信装置に対して、識別情報を送信する情報通信装置であって、前記第1及び第2の通信装置が前記電子データを伝送するのに必要な固有の識別情報を保持する識別情報保持手段と、前記第1及び第2の通信装置に対して前記固有の識別情報を送信する通信手段と、を備える。

【0023】

また、本発明は、ネットワークに接続された送信装置と、前記送信装置から送信された、著作権保護のための暗号化を行った電子データを、前記ネットワークを介して受信する受信装置と、を備える通信システムにおいて、前記送信装置及び前記受信装置の少なくとも一方は、識別情報送信装置との間で、前記ネットワークとは異なるインタフェースを介して通信を行い、前記識別情報送信装置から送信された固有の識別情報を受信する通信手段と、受信された前記固有の識別情報を登録する識別情報登録手段と、前記他の通信装置が前記固有の識別情報を登録しているか否かを判断する識別情報登録判断手段と、前記他の通信装置が前記固有の識別情報を登録していると判断される場合に、該他の通信装置との間で、著作権保護のための認証鍵交換を完了させる認証鍵交換処理手段と、を備える。

40

【発明の効果】

【0024】

50



以上詳細に説明したように、本発明によれば、他の通信装置が有限範囲内のネットワークに接続されている場合のみ、該他の通信装置の装置識別情報を登録するため、電子データの伝送先を限定することができ、電子データの著作権保護を確実に図ることができる。

【発明の実施の形態】

【0025】

以下、本発明に係る情報通信装置、通信システム及びデータ伝送制御プログラムについて、図面を参照しながら具体的に説明する。

【0026】

(第1の実施形態)

図1は本発明に係る通信システムの第1の実施形態の概略構成を示すブロック図である。図1の通信システムは、個人宅内で主にAVデータを送受信することを目的としており、ホームネットワーク1に接続された送信装置2及び受信装置3を備えている。 10

【0027】

ホームネットワーク1として、例えばIEEE802.11に準拠した無線LAN、イーサネット（登録商標）またはIEEE1394ネットワークなどの種々のネットワーク形態が採用可能である。ホームネットワーク1には送信装置2や受信装置3以外の装置が接続されていてもよいが、簡略化のため、ここでは省略している。ホームネットワーク1上でインターネットプロトコル（IP）が使用されている場合、IPv4でもよいし、IPv6でもよい。

【0028】

送信装置2と受信装置3との間で送受信されるAVデータは、著作権保護が必要なAVデータであり、適切な著作権保護を施した状態で転送される。本実施形態では、ネットワーク上の著作権保護を実現する方式として、DTCPを仮定するが、DTCP以外の著作権保護の仕組みを採用してもよい。なお、DTCPについては、<http://www.dtcp.com>を参照されたい。 20

【0029】

本実施形態では、送信装置2と受信装置3との間で、あらかじめ「登録」の手順を設け、互いの装置、あるいは、一方の装置が他方の装置を「登録」する。この「登録」が終了していない装置間では、AVデータの伝送、暗号化されたAVデータの復号化、及び認証・鍵交換処理の完了を許可しない、という仕組みを導入する。

【0030】

具体的には、異なるホームネットワーク1間では、パケットの伝送に時間がかかることが多く、また異なるホームネットワーク1同士を接続する場合、通常はルータ網（公衆インターネット）が間に入る等の特性を利用して、登録用のパケットの交換が一定時間以内に終了しない場合には、登録を完了させる。また、登録に用いるパケットとして、IPパケットでなく、物理ネットワークレイヤ等のパケット（例えば、イーサネット（登録商標）パケットや無線レイヤパケット）を用いる。 30

【0031】

図2は送信装置2の一実施形態の概略構成を示すブロック図である。図2の送信装置2は、ネットワークインターフェース部11と、通信処理を実行する通信処理部12と、送信装置2自身のDTCPデバイスIDを記録するDTCPデバイスID記録部13と、ネットワークを介して取得した同じ宅内の他の通信装置のデバイスIDを登録するID管理部14と、ID管理部14にデバイスIDを登録する制御を行う事前登録処理部15と、他の通信装置からデバイスIDが通知されるまでの時間を計測する時計16と、著作権保護を図るためにDTCP認証・鍵交換処理を行う認証・鍵交換処理部17と、送信するデータを暗号化する暗号処理部18と、受信装置3に送信するAVデータやDTCP管理データを通信パケットに変換するパケット処理部19と、AVデータを蓄積するコンテンツ供給部20とを備えている。 40

【0032】

事前登録処理部15は、宅内の他の通信装置にデバイスIDの送信要求を行ってからデバイスIDの応答があるまでの時間を時計16で計測し、その時間が所定時間以内であれば、ID管理部14にデバイスIDを登録する。ID管理部14は、登録されたデバイスIDのリスト（以下、IDリスト）を有し、事前登録処理部15からデバイスIDの登録要求があると、そ 50

のIDがIDリストに登録されていなければ、IDリストに加える。

【0033】

図3はIDリストの一例を示す図である。IDリストは、必須項目として他の通信装置のDTCPデバイスIDを登録し、オプション項目として例えば、RTT (Round Trip Time)、固有ID (例えば、MACアドレス) 及び最終利用日時 (他の通信装置と最後に通信を行った日時) を登録する。

【0034】

IDリストには、N (Nは所定の整数) 個までのデバイスIDを登録することができる。新たなデバイスIDの登録要求があったときに、すでにN個のデバイスIDが登録されている場合には、新たなデバイスIDの登録を拒否するか、あるいは最も長い期間通信を行っていない他の通信装置のデバイスIDか、あるいは最も古くに登録されたデバイスIDを削除して、新規のデバイスIDを登録できるようになっていてもよい。また、ユーザが何らかのユーザインタフェースを介して、任意のデバイスIDを削除できるようにしてもよい。

【0035】

ここで、DTCPデバイスIDとは、DTCPデバイスの識別番号である。全世界のDTCPデバイスは、それぞれ固有のIDをもつのが望ましい。DTCPデバイスIDは、機器証明書 (Certificate) と呼ばれる、「その機器が、正しくライセンスされた機器であることの証明書」の中に含まれるIDでもよい。機器証明書には、デジタル署名等が含まれ、これを検証することにより、正しい機器証明書であるか否かを確認することができる。

【0036】

図4は本発明に係る受信装置3の内部構成を示すブロック図である。図4の受信装置3は、ネットワークインターフェース部21と、通信処理を実行する通信処理部22と、受信装置3自身のDTCPデバイスIDを記録するDTCPデバイスID記録部23と、ネットワークを介して取得した同じ宅内の他の通信装置のデバイスIDを登録するID管理部24と、ID管理部24にデバイスIDを登録する制御を行う事前登録処理部25と、他の通信装置からデバイスIDが通知されるまでの時間を計測する時計26と、著作権保護を図るためにDTCP認証・鍵交換処理を行う認証・鍵交換処理部27と、受信したデータを復号化する暗号処理部28と、受信された信号をAVデータに変換するパケット処理部29と、AVデータを蓄積するコンテンツ供給部30とを備えている。

【0037】

図5及び図6は送信装置2と受信装置3との間で行われる第1の実施形態におけるAVデータの伝送処理手順を示すシーケンス図である。図5及び図6のシーケンス図は、送信装置2と受信装置3の各ユーザが「登録ボタン」を押すか、「登録アイコン」をクリックすることにより開始される (ステップS11、S12)。

【0038】

なお、送信装置2と受信装置3のいずれか一方のみが開始のアクションを行うことで、図5の処理を開始してもよい。あるいは、送信装置2と受信装置3の電源をオンしたときに、自動的に登録モードに設定されて、図5の処理が開始されてもよい。

【0039】

いずれにしても、「登録ボタンを押した装置同士」、あるいは「登録ボタンを押した通信装置とその他の通信装置 (通常は電源がオンしている通信装置)」との間で登録処理が行われることになる。

【0040】

図5では、送信装置2と受信装置3の二装置間での登録について説明したが、同時に3つ以上の通信装置の登録を行ってもよい。

【0041】

登録処理が開始されると、送信装置2は時計による時間計測を開始 (タイマオン) し (ステップS13)、IDリストに登録する目的で、受信装置3に対してデバイスID送信要求パケットを送信する (ステップS14)。このパケットは、イーサネット (登録商標) フレームか無線レイヤフレーム (データリンクレイヤフレームまたは物理レイヤフレーム)

10

20

30

40

50

で送信される。デバイスID送信要求パケットには、送信装置2が選択した乱数やタイムスタンプが含まれている。送信装置2は、デバイスID送信要求パケットをネットワーク上でブロードキャストしてもよい。この場合、イーサネット（登録商標）ブロードキャストアドレスを宛先イーサネット（登録商標）アドレスとして用いる。

【0042】

デバイスID送信要求パケットを受けて、受信装置3は、送信装置2に対してデバイスID応答パケットを送信する（ステップS15）。このデバイスID応答パケットも、イーサネット（登録商標）フレームか無線レイヤフレームで送信される。受信装置3は、送信装置2からのデバイスID送信要求パケットに含まれていた乱数やタイムスタンプをそのままデバイスID応答パケットに含めてもよい。これにより、送信装置2は、どの要求パケットに  
10 対する応答かを知ることができ、時計16による時間計測を行いやすくなる。

【0043】

なお、受信装置3からデバイスID送信要求パケットを送信し、そのパケットを受信した送信装置2がデバイスID応答パケットを受信装置3に送信してもよい。この場合、パケットの応答までの時間計測は受信装置3で行うことになる。

【0044】

送信装置2内の事前登録処理部15は、デバイスID応答パケットが所定時間T以内に受信された場合、受信装置3のデバイスIDをID管理部24に登録し、所定時間T以内に受信されなかった場合、登録失敗と判断して、ID管理部24への登録を行わない（ステップS16）。  
20

【0045】

デバイスIDの登録に失敗した場合、ユーザに対して、「デバイスIDの登録は、もっと近距離で同一リンクレイヤネットワーク上で行う必要がある」ことを通知する必要がある。このため、ユーザに対して、送信装置2及び受信装置3を同じイーサネット（登録商標）スイッチに差込んで登録を行うよう誘導したり、直接イーサネット（登録商標）ケーブルで接続して登録を行うよう誘導したり、ネットワーク上のトラフィックを一時的に少なくするよう（例えば、他の通信装置のAVデータの伝送を止めるよう）誘導したり、送信装置2または受信装置3が起動中の他のアプリケーションを停止して処理負担を軽減するよう誘導したりする。

【0046】

ステップS16の処理が終了した後、今度は受信装置3が時計26による時間計測を開始し（ステップS17）、送信装置2に対してデバイスID送信要求パケットを送信する（ステップS18）。この要求を受けて、送信装置2はデバイスID応答パケットを送信する（ステップS19）。  
30

【0047】

受信装置3は、送信装置2からのデバイスID応答パケットが所定時間T以内に受信された場合には送信装置2のデバイスIDをID管理部に登録し、所定時間T以内に受信されなかった場合は、送信装置2のデバイスIDの登録を行わない（ステップS20）。

【0048】

以上の手順で、送信装置2及び受信装置3は登録モードを終了し（ステップS21、S22）、認証・鍵交換処理を行う（図6のステップS23～S29）。  
40

【0049】

まず、受信装置3は、送信装置2に対して、IPパケットを利用して認証・鍵交換要求を行う（ステップS23）。このとき、自己のデバイスIDもIPパケットに含めて送信する。

【0050】

受信装置3からのIPパケットを受信した送信装置2は、受信装置3のデバイスIDがID管理部14に登録されているか否かを確認し（ステップS24）、確認が取れると、受信装置3に対して、IPパケットを利用して認証・鍵交換要求を行う（ステップS25）。このとき、自己のデバイスIDもIPパケットに含めて送信する。

【0051】

送信装置 2 からの IP パケットを受信した受信装置 3 は、送信装置 2 のデバイス ID が ID 管理部 24 に登録されているか否かを確認し（ステップ S 26）、確認が取れると、送信装置 2 と受信装置 3 との間で、認証・鍵交換を行う（ステップ S 27）。

【0052】

認証・鍵交換が成功すると、送信装置 2 と受信装置 3 はコンテンツ暗号鍵を共有し（ステップ S 28、S 29）、送信装置 2 はコンテンツの暗号化を行う（ステップ S 30）。

【0053】

次に、送信装置 2 は受信装置 3 に対して、暗号化された AV データを RTP または HTTP にて伝送する（ステップ S 31）。この AV データを受信した受信装置 3 は、コンテンツの復号化を行う（ステップ S 32）。

10

【0054】

なお、送信装置 2 と受信装置 3 のいずれか一方で、すでにデバイス ID の登録が終わっている場合には、図 5 のステップ S 13～S 16 または S 17～S 20 を省略してもよい。

【0055】

デバイス ID の登録要求と登録応答を行う際に、なりすまし（man in the middle attack）を防止する手順を設けてもよい。この場合、例えば図 5 のステップ S 14～S 16 の代わりに図 7 のような処理を行う。

【0056】

まず、送信装置 2 は受信装置 3 に対して、イーサネット（登録商標）フレームまたは無線レイヤフレームにて乱数送信パケットを送信する（ステップ S 41）。乱数送信パケットには、送信装置 2 が生成した乱数  $r$  が含まれている。

20

【0057】

この乱数送信パケットを受信した受信装置 3 は、乱数  $r$  と自己のデバイス ID を用いて署名を計算する（ステップ S 42）。次に、受信装置 3 は送信装置 2 に対して、イーサネット（登録商標）フレームまたは無線レイヤフレームにて乱数受信通知を行う（ステップ S 43）。

【0058】

この通知を受けた送信装置 2 は、時計による時間計測を開始し（ステップ S 44）、受信装置 3 に対して、イーサネット（登録商標）フレームまたは無線レイヤフレームにてデバイス ID 要求パケットを送信する（ステップ S 45）。このパケットには、上述した乱数  $r$  が含まれている。

30

【0059】

このパケットを受信した受信装置 3 は、送信装置 2 に対して、乱数  $r$ 、自己のデバイス ID 及び署名を含むデバイス ID 応答パケットを送信する（ステップ S 46）。

【0060】

送信装置 2 は、デバイス ID 要求パケットを送信してからデバイス ID 応答パケットが受信されるまでの時間が所定時間  $T$  以内か否かを判断し、所定時間  $T$  以内であれば、受信装置 3 のデバイス ID =  $b$  を ID 管理部に登録し、所定時間  $T$  以内に受信されなかった場合は、ID 管理部への登録を行わないようにする（ステップ S 47）。

40

【0061】

このように、第 1 の実施形態では、デバイス ID の登録要求を行ってから所定時間以内に応答が返ってきた場合のみ、他の通信装置（受信装置 3 または送信装置 2）の登録を行うようにしたため、有限の範囲内の通信装置との間でのみ AV データの伝送を行うことができ、簡易な処理で AV データの著作権保護を図ることができる。

【0062】

（第 2 の実施形態）

第 2 の実施形態は、受信装置 3 が送信装置 2 に対して認証・鍵交換要求を行った後に、送信装置 2 が受信装置 3 にデバイス ID 要求パケットを送信するものである。

50

## 【0063】

第2の実施形態の送信装置2及び受信装置3は、それぞれ図3及び図4と同様に構成されるため、構成の説明を省略する。

## 【0064】

図8は第2の実施形態におけるAVデータの伝送処理手順を示すシーケンス図である。まず、受信装置3から送信装置2に対して認証・鍵交換要求を行う（ステップS51）。送信装置2は、認証・鍵交換要求を行った受信装置3がID管理部に登録されていないことを確認すると（ステップS52）、時計による時間計測を開始し（ステップS53）、受信装置3に対してイーサネット（登録商標）フレームまたは無線レイヤフレームにてデバイスID要求パケットを送信する（ステップS54）。 10

## 【0065】

このパケットに応答して、受信装置3は、送信装置2に対してイーサネット（登録商標）フレームまたは無線レイヤフレームにてデバイスID応答パケットを送信する（ステップS55）。

## 【0066】

次に、送信装置2は、デバイスID要求パケットを送信してからデバイスID応答パケットが所定時間T以内に返ってきた場合、受信装置3のデバイスID（=b）をID管理部14に登録し、所定時間T以内に返って来なかった場合、登録を行わない（ステップS56）。

## 【0067】

次に、今度は、受信装置3は同様の手順で送信装置2のデバイスIDの登録を行う（ステップS57～S60）。以下、図6のステップS21～S32と同様の処理を行う。 20

## 【0068】

なお、送信装置2と受信装置3のいずれか一方で、すでにデバイスIDの登録手続きが終わっている場合には、図8のステップS52～S56またはS57～S60を省略してもよい。

## 【0069】

このように、第2の実施形態では、認証・鍵交換要求のあった後にデバイスIDの登録要求を行うため、不必要にデバイスIDの登録要求とその応答を行わなくて済み、通信トラフィックを低減できる。

## 【0070】

（第3の実施形態）

第3の実施形態は、第1及び第2の実施形態と異なり、短距離無線装置から送信されたIDを登録している送信装置と受信装置との間でのみAVデータを伝送できるようにしたものである。

## 【0071】

図9は本発明に係る通信装置の第3の実施形態の概略構成を示すブロック図である。図9の通信システムは、図1の構成に加えて、赤外線リモートコントローラ（以下、リモコン）や無線タグなどからなる短距離無線装置4を備えている。

## 【0072】

本実施形態の送信装置2a及び受信装置3aは、それぞれ短距離無線装置4と無線通信を行って、短距離無線装置4から送信されたグローバルユニークなID（以下、短距離IDと呼ぶ）に登録する。この短距離IDが登録されている送信装置2aと受信装置3aの間でのみ、AVデータの伝送が行えるようにする。より具体的には、上述のIDが登録されていない送信装置2aと受信装置3aの間では、認証鍵交換（あるいはコンテンツの送受信）が成功しないようにする。 40

## 【0073】

個々の短距離無線装置4は、短距離IDを保持しており、このIDを、短距離無線通信を利用してのみ、送信装置2aと受信装置3aにそれぞれ送信する。ここで、短距離とは、例えば赤外線を利用する場合には、赤外線が届く範囲（例えば数m）であり、また無線タグを利用する場合には、電波が届く範囲（例えば数cm）である。 50

## 【0074】

図10は図9の送信装置2aの概略構成の一例を示すブロック図である。図10では、図2と共通する構成部分には同一符号を付しており、以下では、図2との相違点を中心に説明する。

## 【0075】

図10の送信装置2aは、図2と同様に、ネットワークインターフェース部11、通信処理部12、DTCPデバイスID記録部13、ID管理部14、DTCP認証鍵交換処理部17、暗号処理部18、パケット処理部19及びコンテンツ供給部20を備えている。この他、図10の送信装置2aは、短距離無線通信のための短距離無線インターフェース部41と、短距離無線装置4との間で認証鍵交換を行う短距離認証鍵交換処理部42と、短距離無線通信により取得した短距離IDを登録する短距離ID管理部43と、短距離ID管理部43に短距離IDを登録する制御とを行う事前登録処理部44と、短距離IDの登録が終了したことをユーザに通知する登録終了通知処理部45と、短距離IDの登録時にのみ短距離無線インターフェース部41やその周辺部に電源電圧を供給する電源制御部46とを備えている。

## 【0076】

短距離ID管理部43と事前登録処理部44はそれぞれ、セキュリティ保持のために、短距離IDを暗号化する暗号通信処理部43a、44aを持ってもよい。これにより、短距離ID管理部43と事前登録処理部44との間のデータバス上で短距離IDを不正に取得されるおそれなくなる。すなわち、短距離無線インターフェース部41、短距離無線認証鍵交換処理部42及び事前登録処理部44などが、例えば、赤外線モジュールや無線タグモジュールなどの形態でモジュール化されていて、各モジュールがPCIバス等の汎用バスに接続されて場合で、かつ短距離ID管理部43やDTCP認証鍵交換処理部17がMPU側のソフトウェア等で処理される場合、事前登録処理部44と短距離ID管理部43との間でのデータ伝送は汎用バスを介して行うことになる。したがって、短距離ID等が暗号化されていないと、このID等を汎用バス上で不正に取得されて、ID等の不正利用や不正コピーなどが行われるおそれがある。

## 【0077】

このことから、短距離ID管理部43と事前登録処理部44にそれぞれ暗号通信処理部43a、44aを設けて、短距離ID等を暗号化して伝送するのが望ましい。なお、暗号通信処理部43a、44aは、ハードウェアで構成してもよいし、ソフトウェアで暗号化するAPIを用意して、ソフトウェアでID等を暗号化してもよい。

## 【0078】

また、この暗号通信処理部43aと44a間でのやり取りが、一定時間以内に行われているかどうかを計測する機能が、これら暗号通信処理部43aと44aに内蔵されていても良い。これは、短距離ID管理部43と事前登録処理部44との物理的な距離が、一定長さ以内（例えば、同じ筐体の中、あるいは、短距離無線の処理部がUSB dongle等の外付け部品として構成されており、この外付け部品と短距離ID管理部43との物理的な距離が一定長さ以内）であることを確認するための機能である。

## 【0079】

この場合の外付け部品とは、例えば、短距離無線インターフェース部41と、短距離認証鍵交換処理部42と、事前登録処理部44とで構成される。この機能がない場合、外付け部品を遠隔地に配置し、短距離ID管理部43と外付け部品との間をインターネット等の公衆網（広域網）で接続して、遠隔地から登録を行う、という攻撃が考えられるので、これを未然に防止する効果がある。

## 【0080】

また、短距離無線に関する機能（例えば、短距離無線インターフェース部41と、短距離認証鍵交換処理部42と、事前登録処理部44）は、短距離IDの登録の時以外には使うことのない機能である可能性がある。このため、これらの機能は、短距離IDの登録時以外には通電しない等の工夫をすることにより、省電力を図ることが可能になる。これを制御するのが電源制御部46である。電源制御部46は、ユーザが短距離IDの登録ボタン

等を押したことを検知して、電源制御を行う。

【0081】

ここで、短距離無線IDとは、短距離無線装置4の識別番号であり、DTCPと同じライセンス機関が、世界唯一の値となるように割り当てる識別番号であってもよい。また、短距離無線IDは、DTCPのデバイスIDと同様に、機器証明書(Certificate)と呼ばれる「その機器が、正しくライセンスされた機器であることの証明書」の中に含まれるIDであってもよい。この機器証明書には、デジタル署名等が含まれ、これを検証することにより、正しい機器証明書であるかどうかを確認することができる。

【0082】

図11は受信装置3aの一実施形態の概略構成を示すブロック図である。図11では、図4と共通する構成部分には同一符号を付しており、以下では、図4との相違点を中心に説明する。

【0083】

図11の受信装置3aは、図4と同様に、ネットワークインターフェース部21、通信処理部22、DTCPデバイスID記録部23、DTCP認証鍵交換処理部27、暗号処理部28、パケット処理部29及びコンテンツ供給部30を備えている。この他、図11の受信装置3aは、短距離無線通信のための短距離無線インターフェース部51と、短距離無線装置4との間で認証鍵交換を行う短距離認証鍵交換処理部52と、短距離無線通信により取得した短距離IDを登録する短距離ID管理部53と、短距離ID管理部53に短距離IDを登録する制御を行う事前登録処理部54と、短距離IDの登録が終了したことをユーザに通知する登録終了通知処理部55と、短距離IDの登録時にのみ短距離無線インターフェース部、あるいはその周辺を稼動する(電源をONにする)電源制御部56とを備えている。

【0084】

図12は送信装置2aや受信装置3a内の短距離ID管理部43、53のデータ構造を示す図である。短距離ID管理部43、53は、短距離IDの値が必須項目として登録され、それ以外に、オプション項目として、各IDごとに、RTT(Round Trip Time)、DTCPデバイスID及び登録日時などが登録される。

【0085】

図13は短距離無線装置4を赤外線リモコン装置で実現した場合の内部構成の一例を示すブロック図であり、赤外線リモコン装置の例を示している。図13の赤外線リモコン装置は、赤外線通信インターフェース部61と、AV機器を初期化するためのAV機器初期化処理部62と、AV機器を制御するためのAV機器制御処理部63と、自装置の短距離IDを記録する短距離ID記録部64と、短距離ID記録部64にIDを登録する制御を行う事前登録処理部65と、短距離ID記録部64に短距離IDを記録した回数を計測する登録回数カウンタ66と、送信装置2a及び受信装置3aとの間で認証鍵交換を行う短距離無線認証鍵交換処理部67と、ユーザインタフェース部68とを備えている。

【0086】

ここで、赤外線通信インターフェース部61は、短距離ID登録用双方向赤外線インターフェース61aと、AV機器制御用片方向赤外線インターフェース61bとを内蔵していてもよい。これは、AV機器を制御するための赤外線リモコンのインターフェースは一般に片方向であるのに対して、後述するように本実施形態の短距離IDを登録するための赤外線インターフェースは双方向である。これら2つの機能を実現するためには、赤外線通信インターフェース部61は、2つの赤外線インターフェース61aと61bを備える必要がある。これらの2つの赤外線インターフェースは、2つ以上の個別部品で構成されていても良いし、1つの個別部品に封止されていても良い。短距離ID登録用双方向赤外線インターフェース61aは短距離無線認証・鍵交換処理部67とAV機器初期化処理部62と接続している。一方、AV機器制御用片方向赤外線インターフェース61bは、AV機器制御処理部63と接続されている。これら2つの赤外線インターフェース61a、61bは、異なる赤外線の周波数や、コマンド体系、パケットフォーマット等を使用してもよい。

【0087】

10

20

30

40

50

一方、図14は短距離無線装置4を無線タグ装置で実現した場合の内部構成の一例を示すブロック図である。図14の無線タグ装置は、無線タグ通信インターフェース部70と、AV機器初期化処理部71と、短距離無線認証鍵交換処理部72と、事前登録処理部73と、登録回数カウンタ74と、短距離ID記録部75と、ユーザインタフェース部76とを備えている。

【0088】

無線タグ装置は、受信電波により生成された電力を利用して無線信号を送信するため、バッテリーが不要となり、経済的である。図14では省略しているが、無線タグ装置内には、受信電波により生成された電力を蓄積するキャパシタが設けられている。

【0089】

図15は送信装置2a及び受信装置3aにおける短距離IDの登録処理手順を示すシーケンス図である。以下、図15に基づいて短距離IDの登録処理手順を説明する。短距離無線装置4から送信装置2a（または受信装置3a）に短距離IDを送信する際、ユーザが短距離無線装置4の図13に示すボタン68aを押下すると、短距離無線装置4は登録モードに入る（ステップS71）。また、ユーザは、短距離IDを送信すべき対象である送信装置2a（または受信装置3a）のボタンも押下し、短距離無線装置4を送信装置2a（または受信装置3a）に向ける。以上の手順により、送信装置2a（または受信装置3a）は登録モードに入る（ステップS72）。

【0090】

この登録モードに入った場合に、電源制御部56（または66）は、送信装置2a（または受信装置3a）における短距離無線インタフェース部41（または51）およびその周辺部を通電するようにしてもよい。

【0091】

このように、本実施形態では、短距離IDの登録を行う際、ユーザ自身が送信装置2aや受信装置3aのボタンを押下する必要があるため、送信装置2aから離れた場所にいる受信装置3aに、インターネット等を介してAVデータを送信するおそれなくなる。

【0092】

次に、ユーザは、短距離無線装置4を送信装置2a（または受信装置3a）に向けるか近づけて、短距離ID登録ボタンを押下する（ステップS73）。これにより、短距離無線装置4と送信装置2a（または受信装置3a）との間で認証鍵交換が行われ、正規のライセンス機関が認めた装置であることを互いに認証する（ステップS74）。その際、必要に応じて、公開鍵などの鍵交換も行う。この手順は、後に詳述する。

【0093】

次に、短距離無線装置4は、短距離IDを送信装置2a（または受信装置3a）に送信して登録を行った回数を計測する登録回数カウンタがゼロより大きいかな否かを判断する（ステップS75）。登録回数カウンタがゼロより大きければ、所定回数以下の登録しか行っていないことを示しており、この場合は送信装置2a（または受信装置3a）に短距離IDを送信する（ステップS76）。登録回数カウンタがゼロの場合には、所定回数の登録をすでに行ったことを示しており、この場合は短距離IDの送信を中止する。

【0094】

短距離無線装置4は、送信装置2a（または受信装置3a）に短距離IDを送信した場合には、登録回数カウンタを「1」だけデクリメントする（ステップS77）。

【0095】

短距離IDを受信した送信装置2a（または受信装置3a）は、その短距離IDを短距離ID管理部43、53に伝送する（ステップS78）。伝送途中で短距離IDを不正取得されないように、上述したように、例えば短距離IDを暗号化したり、署名を付けて改ざんされたかな否かを確かめ確認できるようにしてもよい。また、この短距離ID管理部43、53への伝送が一定時間以内に行われたかどうかの測定を行っても良い。

【0096】

次に、短距離ID管理部43、53に登録されている短距離IDの数が所定数N未満かな否か

10

20

30

40

50



を確認し（ステップS79）、所定数以下であれば、受信された短距離IDの登録を行う。一方、すでに所定数Nの短距離IDが登録されている場合には、上述したように、最も長い間登録された短距離IDを削除するなどして、新たな短距離IDを登録してもよい。

#### 【0097】

以上の手順により、短距離無線装置4と送信装置2a（または受信装置3a）での登録モードを終了し、終了した旨をビープ音やディスプレイ上への表示等によりユーザに通知する（ステップS80～S83）。

#### 【0098】

送信装置2aと受信装置3aは、それぞれが所持する短距離ID管理部43、53に短距離IDを登録している。短距離ID管理部43、53には、予め定めた所定個数NまでのIDを登録することができる。N個の値は1でもよいが、例えば4、8及び16などの数値が選択されてもよい。仮に、上限であるN個まですでに登録されている状態で、新たなIDの登録要求があった場合には、最も過去に登録されたIDを削除する代わりに、新規のIDを登録するなどの手法も考えられるが、所定個数NのIDを登録すると、それ以上の登録はできないというのが基本的な考え方である。

#### 【0099】

短距離ID管理部43、53への登録処理は、送信装置2aと受信装置3aがそれぞれ個別に行う。すなわち、送信装置2aと受信装置3aのそれぞれが、同じ短距離無線装置4を使用して短距離IDの登録を行う。この場合、送信装置2aと受信装置3aが互いに近距離にいることを確認できると、さらに望ましい。このような確認ができないと、送信装置2aは東京にあり、受信装置3aが大阪にある場合でも、異なる時間に同じ短距離無線装置4を用いて、同じ短距離IDを登録できてしまい、任意の遠隔地同士での遠隔通信が可能になる。

#### 【0100】

このため、図13に示すように、短距離無線装置4内に時計69を設け、送信装置2a及び受信装置3aの登録作業は連続して数分以内に行わないと無効になるようにしてもよい。

#### 【0101】

あるいは、短距離無線装置4内にGPS（Global Positioning System）を内蔵し、送信装置2aと受信装置3aとの距離が所定長さ以上離れていると予測できる場合は、短距離IDの登録ができないようにしてもよい。

#### 【0102】

また、図10および図11に示すように、送信装置2aと受信装置3aの事前登録処理部44、54にRTT（Round Trip Time）を計測するRTT計測部47、57をそれぞれ設け、リモコン装置や無線タグ装置とのデータのやり取りに要する時間（RTT）が、一定時間以下で行われている事を確認し、そうでない場合には短距離IDの登録ができないようにしてもよい。RTT計測部47、57は、例えば短距離無線装置4に対して特定のパケットを送信し、これに対する応答パケットが返ってくるまでのラウンドトリップ時間を計測する。この計測結果に基づいて、短距離無線装置4までの距離が推定される。

#### 【0103】

また、送信装置2aと受信装置3aの事前登録処理部44、54にそれぞれ時計を設け、リモコン装置や無線タグ装置とのデータのやり取り（RTT）が、一定時間以下で行われている事を確認し、そうでない場合には短距離IDの登録ができないようにしてもよい。

#### 【0104】

図16は認証鍵交換および登録用短距離ID送信処理のシーケンス図である。まず、短距離無線装置4から送信装置2a（又は受信装置3a）に対して、登録処理の開始を要求するトリガをかける（ステップS111）。すると、送信装置2a（または受信装置3a）の事前登録処理部44、54は、RTT計測部47、57内のタイマをスタートさせ（ステップS112）、ラウンドトリップ時間（RTT）を測定するためのコマンドを短距離無線

装置 4 に対して送信する (ステップ S 1 1 3)。このコマンドには、短距離無線装置 4 が選択したランダム値  $A_n$  が共に伝送されても良い。これを受信した短距離無線装置 4 は、即座にリプライを送信装置 2 a (又は受信装置 3 a) に対して送信する (ステップ S 1 1 4)。このリプライには、送信装置 2 a (又は受信装置 3 a) が選択したランダム値  $B_n$  が共に伝送されても良い。

#### 【0105】

これを受信した送信装置 2 a (又は受信装置 3 a) は、RTT計測部 4 7、5 7 内のタイマを使って、RTTを計測する (ステップ S 1 1 5)。この値が、あらかじめ定めた値 (例えば数 ms) 以下である場合、短距離無線装置 4 と、送信装置 2 a (又は受信装置 3 a) との間が一定距離以下であると認識し、これに続く認証鍵交換処理を有効とする。もし、この RTT が一定時間以上かかった場合には、短距離無線装置 4 と送信装置 2 a (又は受信装置 3 a) との間が一定距離以上 (間に公衆網が介在し、これらの装置が遠隔地に配置されている可能性がある) と認識し、以降の認証鍵交換処理を無効としても良い。この RTT の計測は、暗号演算やハッシュ演算が発生しないシーケンスにて行っている。このため、暗号演算やハッシュ演算に必要な時間を考慮することなく、厳密な値に近い RTT の値を計測できる、というメリットがある。

#### 【0106】

なお、本実施形態においては、送信装置 2 a (又は受信装置 3 a) の側が RTT の計測を行っているが、例えばシーケンスの向きを逆にして、短距離無線装置 4 の側が RTT の計測を行うようにしても良い。また、送信装置 2 a (又は受信装置 3 a) と、短距離無線装置 4 の全てが RTT の計測を行うような手順も考えられる。

#### 【0107】

次に、短距離無線装置 4 と送信装置 2 a (又は受信装置 3 a) は、認証鍵交換処理に入る。本実施形態における、この処理は、DTCP標準で既に標準化されている、拡張制限認証 (Extended Restricted Authentication) を用いる事とする。即ち、送信装置 2 a (又は受信装置 3 a) からキー選択ベクトル  $A_{ksv}$  を短距離無線装置 4 に送信し (ステップ S 1 1 6)、短距離無線装置 4 からはその機器証明書 ( $B_{cert}$ ) とキー選択ベクトル ( $B_{ksv}$ ) を送信装置 2 a (又は受信装置 3 a) に送信する (ステップ S 1 1 7)。双方はあらかじめ定められた演算に従って、 $R$ 、及び  $R'$  の値を計算する (ステップ S 1 1 8、S 1 1 9)。

#### 【0108】

ここで、SHA-1とは、あらかじめ定められたハッシュ関数である。短距離無線装置 4 により演算された  $R$  の値は送信装置 2 a (又は受信装置 3 a) に対して送信される (ステップ S 1 2 0)。

#### 【0109】

送信装置 2 a (又は受信装置 3 a) では、自分で計算した  $R'$  と、短距離無線装置 4 から送信されてきた  $R$  の値を比較し (ステップ S 1 2 1)、この値が一致していたならば、認証鍵交換が成功したものと、認証鍵  $K_{auth}$  を演算する (ステップ S 1 2 2、S 1 2 3)。同じ認証鍵の値  $K_{auth}$  を送信装置 2 a (又は受信装置 3 a) も持つことができるため、この値を鍵として、短距離無線装置 4 は短距離 ID の値 ( $AA$ ) を送信装置 2 a (又は受信装置 3 a) に対して送信する (ステップ S 1 2 4)。例えば、短距離 ID と  $K_{auth}$  の値の XOR を使ったり、 $K_{auth}$  の値を鍵とした暗号演算の結果を送ったりする方法が考えられる。

#### 【0110】

DTCPの拡張制限認証には、機器のリボークの仕組みが備わっているため、送信装置 2 a (又は受信装置 3 a) は、特定の短距離無線装置 4 からの手続きを拒否 (リボーク) することが可能である。

#### 【0111】

ここで、DTCPの拡張制限認証の手順の詳細は、<http://www.dtcp.com> の DTCP 標準を参照されたい。

10

20

30

40

50

## 【0112】

図17は送信装置2aと受信装置3aとの間でAVデータの伝送を行う際の処理手順を示すシーケンス図である。ここでは、送信装置2a（デバイスID=aとする）と受信装置3a（デバイスID=bとする）にそれぞれ、短距離ID管理部43、53に共通の短距離ID=AAが登録されているものとする。

## 【0113】

次に、受信装置3aは、自己のデバイスID=bと短距離ID=AAを通知して、送信装置2aに対して認証鍵交換要求を行う（ステップS91）。

## 【0114】

この要求を受信した送信装置2aは、短距離ID管理部に短距離ID=AAが登録されていることを確認し（ステップS92）、自己のデバイスID=aと短距離ID=AAを通知して、受信装置3aに対して認証鍵交換要求を行う（ステップS93）。

10

## 【0115】

この要求を受信した受信装置3aは、短距離ID管理部に短距離ID=AAが登録されていることを確認し（ステップS94）、送信装置2aと受信装置3aとの間で認証鍵交換処理を行う（ステップS95）。

## 【0116】

認証鍵交換に成功すると、送信装置2aと受信装置3aはコンテンツ暗号鍵を共有する（ステップS96、S97）。この鍵を利用して、送信装置2aはAVデータを暗号化し（ステップS98）、暗号化されたAVデータを受信装置3aに送信する（ステップS99）。受信装置3aは、受信したAVデータをコンテンツ暗号鍵を用いて復号する（ステップS100）。

20

## 【0117】

なお、ここでコンテンツ暗号鍵の演算に、短距離IDの値を入力として用いる方法も考えられる。

## 【0118】

図18は、上述したステップS91で受信装置3aから送信された短距離ID=AAが送信装置2aの短距離ID管理部43に登録されていなかった場合の処理手順を示すシーケンス図である。この場合、送信装置2aは、短距離ID管理部43に短距離ID=AAが登録されていないことを確認して、ビープ音等により、ユーザに短距離IDの登録を促す（ステップS101）。

30

## 【0119】

図19は送信装置2aと受信装置3aとの間でAVデータの伝送を行う際の処理手順を示すシーケンス図の別例を示している。この例では、送信装置2aと受信装置3aの間でコンテンツ暗号鍵を共有するまでの処理（ステップS131～S134）は、図17のDTCP認証鍵交換と同様であり、その後、短距離IDの値の確認を片方、あるいは双方で行う（ステップS135～S138）。この場合には、従来のDTCP認証鍵交換の手順に変更が加わらないため、短距離IDの値のやり取りを行う追加のコマンドを用意するのみで、従来のコマンドはそのまま利用できるというメリットがある。

## 【0120】

40

## （第4の実施の形態）

第3の実施形態では、短距離無線装置を介してIDの登録を行うが、第4の実施形態では、短距離無線装置を使う代わりに、ICカード（接触型ICカード）やメモリカード等の着脱可能な記憶装置を使ってIDの登録を行う。ここでICカードとは、ICを内蔵した、例えばプラスチックカードであり、クレジットカード大のものや切手大のものなどが考えられる。また、メモリカードとは、例えば、PCMCIAのメモリカード、あるいはSDカードやメモリスティックに代表されるメモリカード等である。形状はカード形状にかかわらず、例えばUSBキーなどの着脱可能な記憶装置であればよい。

## 【0121】

図20は本発明に係る通信装置の第4の実施形態の概略構成を示すブロック図、図21

50

は図20の送信装置2bの内部構成の一例を示すブロック図、図22は図20の受信装置3bの内部構成の一例を示すブロック図である。第3の実施の形態との差分点は、赤外線リモコンや無線タグなどからなる短距離無線装置の代わりに、ICカード又はメモリカード（以下、総称してICカードと記載）5を用いてIDの登録を行う点である。

#### 【0122】

本実施形態の送信装置2b及び受信装置3bは、第3の実施形態の送信装置2a及び受信装置3aと比べて、短距離無線インタフェース及び短距離無線認証鍵交換処理部がない代わりに、ICカードインタフェース部31、32及びICカード認証鍵交換処理部33、34をそれぞれ有する（図21、図22）。

#### 【0123】

送信装置2bと受信装置3bは、対応するICカードインタフェース部31、32を介してICカード5と通信を行って、ICカード5から送信されたグローバルユニークなID（短距離ID）を登録する。この短距離IDが登録されている送信装置2bと受信装置3bの間でのみ、AVデータの伝送が行えるようにするのは第3の実施形態と同様である。

#### 【0124】

個々のICカードは、短距離IDを保持している。この短距離IDを、送信装置2b、あるいは受信装置3bのICカードスロット（ICカードインタフェース部）に挿入（あるいはセット）し、送信する。IDの送信は、ICカードがICカードインタフェース部に物理的に存在する場合にのみなされるため、遠距離からの登録は不可能であると考えられる。

#### 【0125】

図23はICカードの内部構成の一例を示すブロック図である。図23のICカードは、ICカードインタフェース部81と、AV機器を初期化するためのAV機器初期化処理部82と、自装置の短距離IDを記録する短距離ID記録部83と、短距離ID記録部83にIDを登録する制御を行う事前登録処理部84と、短距離ID記録部83に短距離IDを記録した回数を計測する登録回数カウンタ85と、送信装置2b及び受信装置3bとの間で認証鍵交換を行う短距離無線認証鍵交換処理部86とを有する。

#### 【0126】

図23のICカードはメモリカードやその他の機能を行うものであってもよく、その場合は、メモリ部や他の処理を行う機能がICカードに搭載される。

#### 【0127】

第4の実施形態における短距離IDの登録処理手順や登録のシーケンスや内部の動作等は第3の実施形態と同様であり、第3の実施形態と同様の作用効果が得られる。

#### 【0128】

##### （第5の実施の形態）

第4の実施形態で詳述したIDの登録は、ICカードやメモリカードを介して行っていた。デジタルAV機器の中には、あらかじめICカードのインタフェース部を持ち、「ICカードが刺さっていないと、AV機器として利用できない」機器が存在する。この例が、日本のデジタル放送で広く使われている「B-CASカード」である。このカードには、デジタル放送で送信されてくる（スクランブルがかかった）コンテンツが入力され、このスクランブルを解除して平文のコンテンツにした上で、出力する機能が備わっていたり、内蔵されているID番号（短距離IDとは異なるID）を使って、受信者の確認に使う等の機能が備わっている。

#### 【0129】

デジタル放送機器には、このICカードインタフェース部が必ず備わっており、本発明の短距離IDを書き込むためのICカードと共用できると便利である。本実施形態は、これを実現するものである。

#### 【0130】

図24は本発明に係る通信システムの第5の実施形態の概略構成を示すブロック図、図25は図24の受信装置3cの内部構成の一例を示すブロック図である。図24の通信システムは、図20の通信システムがICカード（又はメモリカード）を使っていたのに対

10

20

30

40

50

し、図 25 では B-CAS カードを用いている点である。

【0131】

図 24 の通信システムは、送信装置 2c と、受信装置 3c と、送信装置 2c や受信装置 3c に挿入可能な B-CAS カード 6 とを備えている。

【0132】

本実施形態では、受信装置 3c がデジタル放送受信機能付の機器（例えばディスプレイ）である場合について説明する。

【0133】

図 25 に示すように、受信装置 3c は、B-CAS カードインタフェース部 35 と、B-CAS カード認証・鍵交換処理部 36 とを有する。送信装置 2c も、B-CAS カードインタフェース部や B-CAS カード認証・鍵交換処理部を持っていたりもよい。

10

【0134】

B-CAS カードインタフェース部 35 は、短距離 ID の登録のための機能を持つ他に、先に述べた B-CAS カード特有の機能（スクランブル処理や受信者確認等）を有する。

【0135】

図 26 は B-CAS カード 6 の内部構成の一例を示すブロック図である。図 26 の B-CAS カードは、B-CAS カードインタフェース部 91 と、B-CAS 処理部 92 と、AV 機器初期化処理部 93 と、短距離無線認証・鍵交換処理部 94 と、事前登録処理部 95 と、登録回数カウンタ 96 と、短距離 ID 記録部 97 とを有する。

20

【0136】

B-CAS カード 6 は、第 4 の実施形態で説明した IC カードと異なり、B-CAS カード特有の機能（スクランブル処理や受信者確認等）を実現する B-CAS カードインタフェース 91 と、B-CAS 処理部 92 とを有する。

【0137】

短距離 ID の登録処理手順や登録のシーケンス、内部の動作等は第 3、第 4 の実施形態と同様である。

【0138】

このように、第 3～第 5 の実施形態では、短距離無線装置 4 が送信装置 2 と受信装置 3 の双方に短距離 ID を登録した場合のみ、送信装置 2 から受信装置 3 に AV データを送信できるようにしたため、特定の送信装置 2 及び受信装置 3 の間でのみ、AV データの伝送を許容することができ、AV データの著作権保護を確実に図ることができる。

30

【0139】

また、短距離無線装置 4 から送信装置 2（または受信装置 3）に短距離 ID を登録可能な回数を制限することにより、短距離無線装置 4 の不正使用による AV データの不正取得を防止できる。

【0140】

さらに、送信装置 2 と受信装置 3 に短距離 ID を登録する時間間隔を所定時間に設定することにより、遠隔地にある送信装置 2 または受信装置 3 への短距離 ID の登録を禁止できる。

【0141】

また、短距離無線装置 4 から送信装置 2（または受信装置 3）に短距離 ID を送信する際に、ユーザが送信装置 2（または受信装置 3）に近づいてボタン操作などを行わないと、短距離 ID の登録ができないようにすることで、ユーザの近くにある送信装置 2（または受信装置 3）のみ登録を許可することができる。

40

【0142】

上述した各実施形態では、著作権保護を図る必要のある AV データの伝送について説明したが、本発明は、著作権保護を図る必要のある各種のコンテンツ（電子データ）の伝送に適用可能である。

【0143】

図 2 等で説明した送信装置 2、2a、2b、2c 及び受信装置 3、3a、3b、3c の

50

内部構成は一例であり、上述した送信装置は受信装置3の機能を備えていてもよいし、逆に上述した受信装置は送信装置の機能を備えていてもよい。

【図面の簡単な説明】

【0144】

【図1】本発明に係る通信システムの概略構成を示すブロック図。

【図2】送信装置の一実施形態の概略構成を示すブロック図。

【図3】IDリストの一例を示す図。

【図4】本発明に係る受信装置の内部構成を示すブロック図。

【図5】送信装置と受信装置との間で行われる第1の実施形態におけるAVデータの伝送処理手順を示すシーケンス図。

10

【図6】図5に続くシーケンス図。

【図7】デバイスIDの登録要求と登録応答を行う際に、なりすましを防止する処理手順を示すシーケンス図。

【図8】第2の実施形態におけるAVデータの伝送処理手順を示すシーケンス図。

【図9】本発明に係る通信装置の第3の実施形態の概略構成を示すブロック図。

【図10】図9の送信装置の一実施形態の概略構成を示すブロック図。

【図11】受信装置の一実施形態の概略構成を示すブロック図。

【図12】送信装置や受信装置内の短距離ID管理部のデータ構造を示す図。

【図13】短距離無線装置を赤外線リモコン装置で実現した場合の内部構成の一例を示すブロック図。

20

【図14】短距離無線装置を無線タグ装置で実現した場合の内部構成の一例を示すブロック図。

【図15】送信装置及び受信装置における短距離IDの登録処理手順を示すシーケンス図。

【図16】認証鍵交換および登録用短距離ID送信処理のシーケンス図。

【図17】送信装置と受信装置との間でAVデータの伝送を行う際の処理手順を示すシーケンス図。

【図18】上述したステップS91で受信装置から送信された短距離ID=AAが送信装置の短距離ID管理部に登録されていなかった場合の処理手順を示すシーケンス図。

【図19】送信装置と受信装置との間でAVデータの伝送を行う際の処理手順を示す別例のシーケンス図。

30

【図20】本発明に係る通信装置の第4の実施形態の概略構成を示すブロック図。

【図21】図20の送信装置の内部構成の一例を示すブロック図。

【図22】図20の受信装置の内部構成の一例を示すブロック図。

【図23】ICカードの内部構成の一例を示すブロック図。

【図24】本発明に係る通信システムの第5の実施形態の概略構成を示すブロック図。

【図25】図24の受信装置の内部構成の一例を示すブロック図。

【図26】B-CASカードの内部構成の一例を示すブロック図。

【符号の説明】

【0145】

1 ホームネットワーク

40

2 送信装置

3 受信装置

11 ネットワークインタフェース部

12 通信処理部

13 DTCPデバイスID記録部

14 ID管理部

15 事前登録処理部

16 時計

17 認証・鍵交換処理部

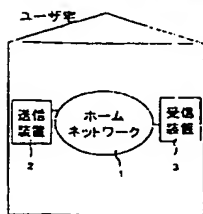
18 暗号処理部

50

1 9	パケット処理部	
2 0	コンテンツ供給部	
2 1	ネットワークインタフェース部	
2 2	通信処理部	
2 3	DTCPデバイスID記録部	
2 4	ID管理部	
2 5	事前登録処理部	
2 6	時計	
2 7	認証・鍵交換処理部	
2 8	暗号処理部	10
2 9	パケット処理部	
3 0	コンテンツ処理部	
4 1	短距離無線インタフェース部	
4 2	短距離無線認証・鍵交換処理部	
4 3	短距離ID管理部	
4 4	事前登録処理部	
4 3 a、4 4 a	暗号通信処理部	
4 5	登録終了通知処理部	
5 1	短距離無線インタフェース部	
5 2	短距離無線認証・鍵交換処理部	20
5 3	短距離ID管理部	
5 4	事前登録処理部	
5 3 a、5 4 a	暗号通信処理部	
5 5	登録終了通知処理部	
6 1	赤外線通信インタフェース部	
6 2	AV機器初期化処理部	
6 3	AV機器制御処理部	
6 4	短距離ID記録部	
6 5	事前登録処理部	
6 6	登録回数カウンタ	30
6 7	短距離無線認証・鍵交換処理部	
6 8	ユーザインタフェース部	
6 9	時計	
7 0	無線タグ通信インタフェース部	
7 1	AV機器初期化処理部	
7 2	短距離無線認証・鍵交換処理部	
7 3	事前登録処理部	
7 4	登録回数カウンタ	
7 5	短距離ID記録部	
7 6	ユーザインタフェース部	40
7 7	時計	

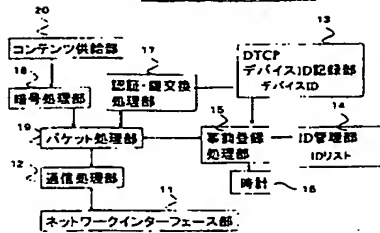
【図 1】

第1の実施形態の概略構成



【図 2】

送信装置の内部構成



【図 3】

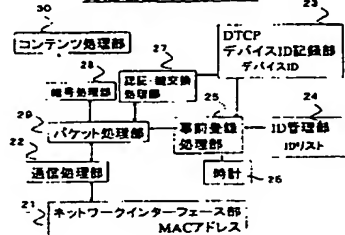
ID管理部内のデバイスIDリスト

必須項目	オプション項目	
対向機器1 デバイスID	RTT OOms	固有ID XXX 最終利用日時 △月×日○時×分
対向機器2 デバイスID	△△ms AA	YYY ×月○日△時○分
対向機器3 デバイスID	××ms BB	ZZZ △月×日○時○分
...	...	...

リストは、N個までのデバイスIDの記録が可能。N+1個目の対向機器から登録要求があった場合には、最近使っていない機器、あるいは、PPO形式で登録した機器を削除して、新規対向機器を登録する。

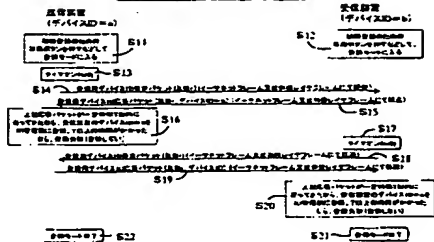
【図 4】

受信装置の内部構成



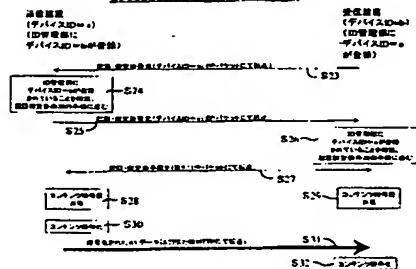
【図 5】

第1の実施形態のAV伝送手順



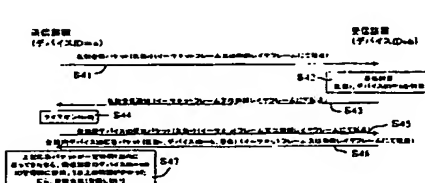
【図 6】

第1の実施形態のAV伝送手順



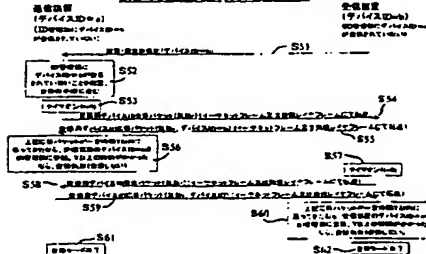
【図 7】

なりすまし防止



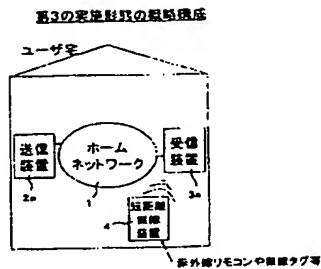
【図 8】

第2の実施形態のAV伝送手順

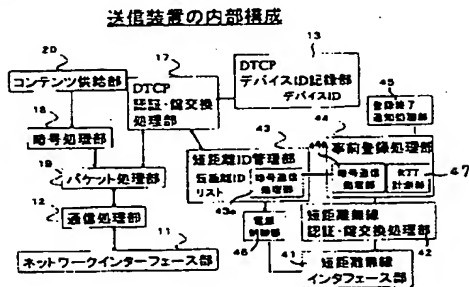




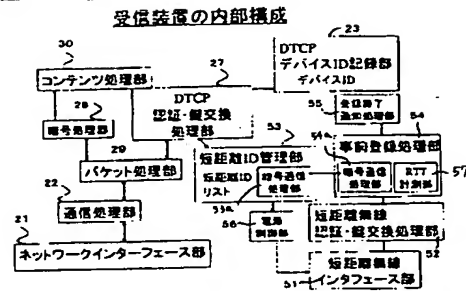
【图 9】



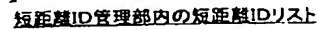
【 10 】



【 1 1 】



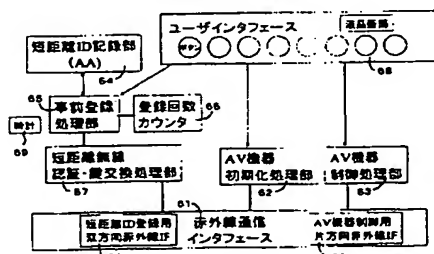
【圖 1 2】



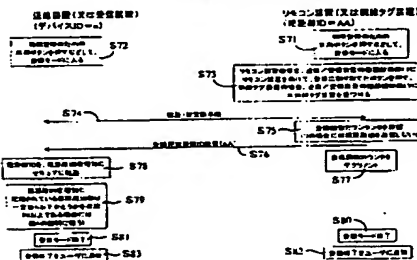
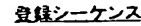
必須項目	オプション項目
(1) 短距離ID=AA	RTT DTCデバイスID 登録日時 ○○ms XXX Δ月×日○時×分
(2) 短距離ID=BB	ΔΔms YYY ×月○日Δ時○分
(3) 短距離ID=CC	×ms ZZZ Δ月×日○時○分
...	

リストは、N個までの登録番号IDの記録が可能。N+1個目の登録番号があった場合には、最近使っていない登録番号、あるいは、FIFO方式で最初に登録した登録番号IDを削除して、新規登録番号IDを登録する。

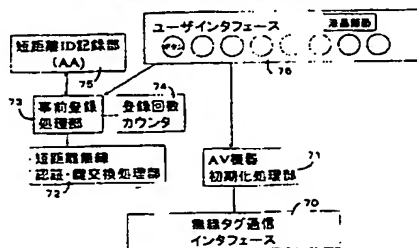
【 例 1 3 】



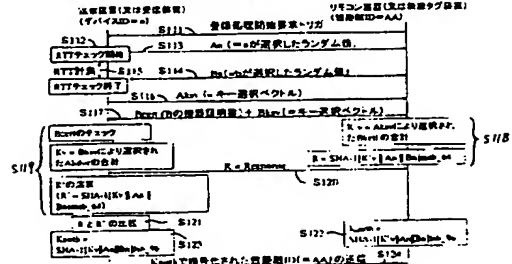
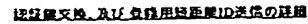
【 15 】



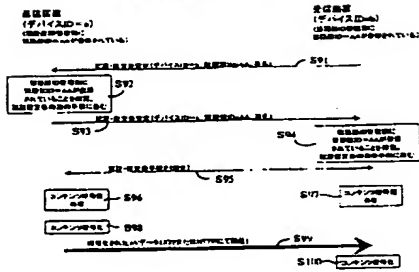
【 図 1 4 】



【 図 1 6 】



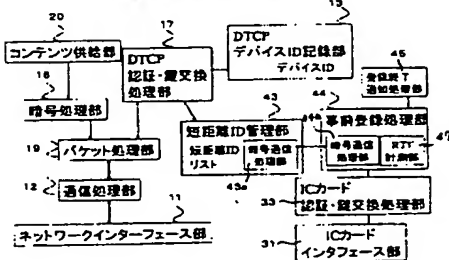
【図 17】 DTCP通信シーケンス



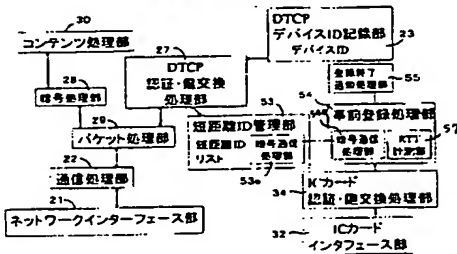
【図 18】 DTCP通信シーケンスの別例



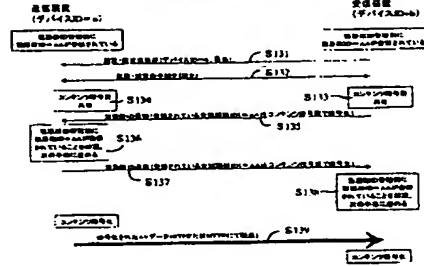
【図 21】 送信装置の内部構成



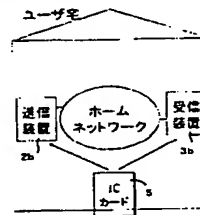
【図 2 2】受信装置の内部構成



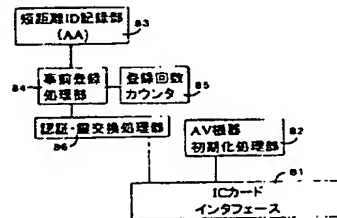
【図 19】 DTCP通信シーケンスの別例



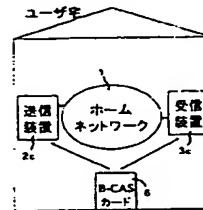
【図 20】  
第4の実施形態の全体構成



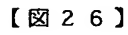
【図 2 3】 ICカードの内部構成



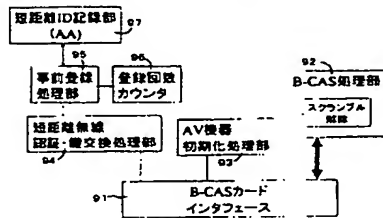
【図 24】  
第5の実施形態の全体構成



### 受信装置の内部構成



### B-CASカードの内部構成



## フロントページの続き

(51) Int. Cl.<sup>7</sup>

H 0 4 L 9/32

F I

G 1 1 B 20/10

H

H 0 4 L 9/00 6 7 5 A

テーマコード (参考)

(72) 発明者 齊 藤 健

神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝研究開発センター内

(72) 発明者 磯 崎 宏

神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝研究開発センター内

(72) 発明者 松 下 達 之

神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝研究開発センター内

(72) 発明者 加 藤 拓

東京都府中市東芝町 1 番地 株式会社東芝府中事業所内

(72) 発明者 上 林 達

神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝研究開発センター内

F ターム (参考) 5B017 AA06 CA16

5B085 AA08 AE29 BA06 BG02 BG04 BG07

5D044 AB07 BC01 BC04 BC05 CC01 CC04 CC08 DE49 GK12 GK17

HH15 HL08 HL11

5J104 AA03 AA07 AA12 AA16 EA04 EA18 JA03 KA02 KA04 KA06

NA02 NA05 NA37 NA38 PA07